BILL LOCKYER
Attorney General

State of California
DEPARTMENT OF JUSTICE

1300 I STREET, SUITE 125
P.O. BOX 944255
SACRAMENTO, CA 94244-2550

Facsimile: (916) 327-7892

February 24, 2000
Little Hoover Commission
Government Technology Hearing

Attorney General Bill Lockyer
Written Testimony

Introduction:

Thank you Mr. Chairman and commission members for the opportunity to provide testimony on information technology in state government.

As Attorney General of California, my office has the responsibility to assist city, county, state, federal and international criminal justice agencies to ensure the uniformity and adequacy of enforcement of California state laws. To support California=s local law enforcement community, my office coordinates statewide narcotics enforcement efforts, participates in criminal investigations, provides forensic science, identification and information services and telecommunication support. In addition, the Department establishes and operates projects and programs to protect Californians from fraudulent, unfair, and illegal activities that victimize consumers or threaten public safety, and enforces laws that safeguard the environment and natural resources.

Currently the Department is developing and supporting numerous applications of statewide technology. I will address technology issues as they relate to public safety.

Information technology has assumed an ever increasing role in crime fighting. The development of new technologies and powerful new tools for communication offer unprecedented opportunities to the law enforcement community.

For instance, DNA technology, a process of human cell identification, is demonstrating daily its capacity to transform the criminal justice system. Recently, DNA evidence

was used to solve the almost 20 year-old rape/murder of a young woman from Hayward, California. The alleged perpetrator, whose genetic profile was matched to biological evidence from the crime scene, previously had not been a suspect. Without DNA evidence, this crime may never have been solved.

In my Department, the Division of Criminal Justice Information Services (DCJIS) is responsible for improving the use of information technology to support local law enforcement technology services and addressing problems in technology projects. This division is dedicated to providing accurate, timely and comprehensive criminal justice information for the Department=s client agencies, primarily local police, sheriffs, district attorneys and five western states.

Information technology is also transforming the way in which law enforcement agencies communicate with their officers and with each other. Federal, state and local agencies have formed enforcement task forces that share information on narcotics, violence suppression, sexual predators through numerous systems and networks. The Statewide Integrated Narcotics (SINS) network is an example. With over 1,200 agency members, law enforcement personnel share sensitive investigative and intelligence information on current cases and subjects. The location information is geographically mapped for officer safety issues and to prevent or notify when another agency is working a particular case.

As the law enforcement community becomes more interconnected, we face new and unique challenges that must be overcome through inter-agency cooperation. Development of standards for data exchange and communication networks will provide long-term benefits to public safety as demand continues to grow. To that end, my Department continues to work on numerous task forces and committees responsible for, in part, the development of an integrated criminal justice process.

A project that we are currently working on with a technical task force is the Cal-Photo. This project involves the sharing of booking photos and Department of Motor Vehicles photos among law enforcement agencies over the state-owned network. Data standards and network definition will allow an officer in a mobile cruiser to obtain photos for investigation or identification purposes. This is a good example of e-government and system integration for data sharing. This type of project has opened the DOJ network to other forms of data sharing.

The Department of Justice runs a number of critical law enforcement databases in California. The following is a brief summary of the key information technology systems operated and maintained by the Department of Justice to serve local law enforcement.

Department of Justice Information Systems:

California Law Enforcement Telecommunications System:
CLETS is the backbone of the Department of Justice's computer communications network. It is through CLETS that a local officer or deputy sheriff can gain remote access to criminal history, stolen vehicle, outstanding warrants and other critical information. For example, the data provides a means to caution law enforcement officers before approaching a car or its occupants.

CLETS receives an average of 1.4 million messages a day (58,333 per hour, 972 per minute and 16 per second) from the 51,000 terminals connected through its network. CLETS is available 99.9% of the time. This system also provides law enforcement and criminal justice agencies with communication capabilities for administrative and broadcast service messages and provides a means for all California law enforcement agencies to inquire and update files of the Criminal Justice Information System (CJIS). Additionally, CLETS allows access to the Federal Bureau of Identification National Crime Information Center (NCIC), the California Department of Motor Vehicles (DMV) files and allows the states of Oregon and Nevada use the databases.

The state provides computer hardware, switching center personnel, administrative personnel and the circuitry to one point in each county. The local agencies provide the circuitry and equipment that links them to their county termination point. Many local agencies have message switching computer (MSC) systems and computer-aided dispatch (CAD) systems that directly connect to CLETS. In addition, local agencies may have mobile digital terminal (MDT) systems, which allow an officer in the field to obtain information directly through CLETS.

Criminal Justice Information Systems:
CJIS is a computer myriad system that houses unique databases. It provides law enforcement agencies with database information through both CLETS and direct access by personnel.

Stolen Vehicle and Automated Boat System: SVS/ABS contains information about stolen and lost vehicles and vehicle parts. The database provides a rapid method of reporting and identifying stolen vehicles, boats, airplanes and equipment. It also provides law enforcement agencies with information to track stolen property. Currently, the database contains more than 500,000 records.

Automated Criminal History System: ACHS provides complete criminal histories to all criminal justice agencies in California to help apprehension, prosecution, custody and

treatment programs. This information enables law enforcement to determine whether individuals applying for licenses, permits or employment in specified situations have criminal records. ACHS contains more than 12 million automated subject records and more than 7.5 million manual subject records.

Wanted Persons System: WPS contains information regarding fugitives for whom law enforcement agencies have issued an arrest warrant. The information provides personal descriptions, alias names and the offense for which the warrant was issued. Officers inquire into WPS to quickly determine if an individual has any warrants, for such categories as failure to appear, escaped, or armed and dangerous. Currently, the database contains more than 700,000 records.

Missing and Unidentified Persons System: MUPS contains information on missing and unidentified persons: physical descriptors, vehicles and suspect information. Law enforcement agencies electronically send, via CLETS, reports of their missing and unidentified persons to the DOJ and the National Crime Information Center (NCIC). Once a local law enforcement agency enters a case, all law enforcement agencies nationwide have access to the information. The database contains more than 27,000 records.

Automated Firearms Systems: AFS provides information on firearms reported as stolen, lost, pawned, purchased or licensed as a concealed weapon, and contains more than 8 million records.

Automated Property Systems: APS provides information on serialized property and persons selling or pawning property through pawnshops and secondhand dealers. This database contains more than 710,000 records.

Automated Child Abuse System: ACAS is a central index that contains information on child abuse victims and suspected abusers for use by law enforcement and child protection agencies. This database contains more than 1.5 million records.

Restraining Order System: ROS contains information on persons named in domestic violence restraining orders who are prohibited from purchasing a firearm. Law enforcement agencies have update and inquiry capability to this database. The database contains more than 132,000 records.

Supervised Release File: SRF provides law enforcement access to an index of subjects on parole or probation that are required to register as sex offenders or arsonists, or considered career criminals. This database contains more than 429,000 records.

Firearms Eligibility Applicant File: FEA contains applicant record information on peace officers, certain security guards and Carry Concealed Weapon (CCW) applicants that the Department of Justice clears for firearms eligibility. When a firearm prohibiting update occurs on the Wanted Persons, Restraining Order and/or Mental Health Firearms Prohibition Systems, a subsequent notification to the contributing agency is sent. The database contains more than 376,000 records.

Mental Health Firearms Prohibition System: NFE contains information on voluntary and involuntary mental health and juvenile firearm prohibition reports, along with other prohibitive firearm files. This is an on-line database with statewide inquiry capability and contains more than 512,000 records.

Other Criminal Justice Databases or Systems:

Violent Crime Information Network: VCIN provides law enforcement with a means to identify and track violent criminals within the state. It is a single source of information for assisting state and local authorities in the investigation of known violent criminal activities and potential suspects. Additionally, this information is available to officers in the field to provide a Aknown-to-VCIN@ response at the time of routine stops. With this information, the officer making the stop can identify a potentially dangerous situation and determine if further questioning is necessary.

California Firearms Information System: CFIS is used to decide a person=s eligibility to purchase firearms. Gun dealers use a Positive Sale Device (PSD) or 800 number to enter gun sales to the CFIS database. This transaction automatically starts the basic firearm eligibility check (BFEC) that uses DIAL (DOJ=s Integrated Access Link) to send inquiries to other state and national databases to determine if the person is on any of these other databases. When the record is approved, Automated Firearms System (AFS) is updated. The record then resides on CFIS and AFS. CFIS has eliminated the paper process for 340,000 firearms sales annually and has been successful in reducing total turnaround time to 10 days.

Child Support Information System: CSIS serves the Family Support Divisions of all fifty-eight county District Attorneys. California Parent Locator accesses State and Federal data files through CSIS used to locate absent non-supporting parents and their assets.

Statewide Integrated Narcotics System: SINS enables local, state and federal law enforcement agencies to coordinate narcotics related law enforcement operations. Law enforcement agencies commonly have open investigations on the same suspects, whose criminal activities span multiple jurisdictional lines.

SINS is a sophisticated, integrated system which allows access to narcotics information among law enforcement agencies within California and across the country. The system utilizes mapping technology to track and graphically display all scheduled law enforcement activities, address matches, and incidents reported.

With this information, law enforcement agencies can avoid potentially dangerous conflicting law enforcement operations, such as when one agency organizes a raid of a narcotics ring in which another agency has placed an undercover agent. Moreover, information sharing allows law enforcement agencies to share narcotics case information, increasing the effectiveness of all law enforcement activities.

California Identification System (Cal-ID): Cal-ID is the largest and most sophisticated fingerprint identification system in the world. Through Cal-ID, law enforcement personnel can conduct latent Acold searches@ against a database of known criminals.

The system, which is comprised of five integrated databases, maintains information on criminals: names, known aliases, dates of birth, and physical descriptions as well as digitized fingerprint information for 10 million known criminal offenders. The system can be accessed by local law enforcement from local jurisdictions and provides a computerized image of the fingerprint ridge characteristics of the offender.

DNA Databank:
For several years, prisoners convicted of one of nine different violent felonies have been required to provide a DNA sample to the state upon release. Upon receipt of these samples, the Department of Justice DNA Databank computerizes them and creates profiles that are used for future investigations.

A Acold hit@ occurs when there is evidence discovered at a crime scene, yet there is no suspect. The investigators can run that sample against the profiles in our database, and often discover a suspect. For example, earlier this year, a Acold hit@ identified a suspect in a San Jose rape case who had fled to the Midwest.

The system was terribly neglected and the Department of Justice now is focusing on catching up with the backlog of samples currently at the lab waiting to be analyzed. The DNA Databank will profile about 12,000 samples a month. By July of 2001 there will be about 200,000 profiles of violent criminals in the database. As more profiles are entered into the database, the chance of apprehension is greatly increased.

Websites:
Created to utilize the new Internet/Intranet technologies, websites now allow authorized law enforcement and legal agencies to gain greater access to information. The central location for the websites is the Department of Justice, Hawkins Data Center in Sacramento.

California Gang Identification: Cal-Gang contains critical information on gangs, gang members, firearms, criminal activities and histories, vehicles, and over 150 other-fields of information necessary in solving gang related crimes. With its widespread implementation, this system has a great potential for becoming a national gang system. Cal-Gang=s success has earned it national recognition and many other states have recently deployed this same system.

California Photo Identification: Cal-Photo is a Telecommunication and Information Infrastructure Assistance Program grant-funded demonstration project. Using inexpensive Internet browser technology, Cal-Photo allows law enforcement agencies to exchange photographs with one another in a timely manner. With this technology, law enforcement agencies can search for, locate and obtain photo images from any law enforcement imaging system in the state.

This pilot project has the potential for the rapid search and retrieval of millions of photographs from disparate local and state systems, at relatively low cost, through the use of evolving web technology. Cal-Photo benefits law enforcement by increasing the availability of images relating to violent and recidivistic offenders and critical missing children. The first phase of this project was implemented in September 1998. San Diego and Orange Counties are currently submitting records, which are being included in Cal-Photo.

Arson Information Reporting System: AIRS permits insurers, law enforcement agencies, fire investigative agencies and district attorneys to deposit arson case information in a database within the Department of Justice. The purpose of the database is to identify utilization patterns by individual claimants and the methods of operation of individuals, groups or businesses engaged in the commission of arson.

Challenges:
Over the years, the Department of Justice has faced many challenges in the information technology arena. In attempting to navigate through the fast-paced and ever-changing world of technology, I have taken a leadership role in opening the lines of communication between the Department of Justice and our customer agencies in local law enforcement. We have encountered the following challenges: standardization, integration, cooperation, security and investment in resources.

Standardization:
In order to have accurate and useful information, the many and varied criminal justice entities throughout the state must report data through standard procedures and systems. As leader in public safety information technology, the Department of Justice has worked to increase standardization of information gathering throughout the state by creating task forces.

For example, the increased use of technology in the court system presents a major challenge in standardization. As a clearinghouse for criminal justice information in the state, standard reporting procedures for court information are vital to our collection of data. The Department is actively participating in this dialog through our involvement in the court technology committee.

In addition, the Department has formed a criminal records improvement committee. This committee is comprised of representatives of the courts, district attorneys, public defenders, California Department of Corrections, California Youth Authority, sheriffs, chiefs of police, senate and assembly members and DOJ staff. The charge of the committee is to advise the Attorney General on methods for improving the criminal record process and exploring implementation of an integrated criminal justice system.

Integration:
The challenge of integration is best illustrated through an example. The CJIS databases are only accessed individually and do not interface with each other. If a police officer searches the Automated Firearms System for a particular individual, that individual=s domestic violence restraining order would not appear. The officer would have to search the Restraining Order System separately for that information.

My vision for future integration is for a beat cop on the street to have the capability to make a single query into the DOJ system and to receive all the relevant information on the individual such as fingerprints, photos, criminal history, domestic violence restraining orders, outstanding warrants and firearms records. While we can envision this capability, current technology has not yet afforded us such an opportunity.

Currently DOJ is working to re-engineer criminal justice systems by reducing the numerous individual databases to a singular relational database. Again taking a leadership role, DOJ staff is working on documenting the current systems and exploring the feasibility of an integrated design effort.

One issue that has appeared in the planning process is the necessity of adequate network bandwidth. Increased bandwidth would allow for more data to be

transferred from terminal to terminal, terminal to car and the capability to have voice, video and data on a single network. This project will take several years, and will only be possible with the cooperation of many state and local entities.

Cooperation:
With the large number of criminal justice agencies tracking issues and gathering information, problems of information-sharing and jurisdiction often arise. Questions such as who owns the data, who has access to the data, who has the right to use the data are frequently asked. Federal, state and local agencies are all involved in this issue.

As Attorney General, I am the chairman of Western States Information Network (WSIN) which is responsible for setting policy for dissemination on narcotic information for the 1,081 member law enforcement agencies in 5 states (Hawaii, Alaska, California, Oregon and Washington).

Security:
A significant challenge is the security of network and systems and privacy of the information they store. To that end, the Department of Justice will continue to coordinate its efforts with all law enforcement agencies and the legislature.

Overall, the track record for public safety information technology is very strong. The Department adheres to federal guidelines regarding the maintenance of criminal justice information. Data security is paramount to the Department and we have several measures to ensure the security of our data, such as extensive backup systems. In the future we will continue to value security and work towards increased encryption and data security.

Investment in Resources:
The recruitment and retention of qualified information technology staff continues to challenge the Department=s technology efforts. In an attempt to increase the total benefit package for staff, the DOJ has participated in numerous studies related to pay and compensation of IT personnel with the Department of Personnel Administration. To date, we still experience a selection process where there are very few qualified candidates and applicants for employment opportunities.

Conclusion:
As we advance into the 21st century, information technology will provide us with new tools to better gather, store and analyze criminal justice information. The Department has achieved success in forming cooperative system and policy task forces comprised of state, county, city and other governmental agencies. We must maintain this

important cooperation with other agencies and seek to expand partnerships with other sectors.

While these partnerships are essential to maintaining and expanding the quality services we provide to our client agencies, we must remember that the collection and storage of criminal justice information involves many unique aspects of information technology.

As Attorney General, I look forward to meeting the information technology challenges which face the criminal justice system and embrace the upcoming advances in technology as a resource for a safer and more secure California. Thank you.